Алексей НАБЕРЕЖНЫЙ

Помогите, украли ICQ!

В последнее время именно с такими просьбами к нам стали обращаться и хорошие знакомые, и просто обыкновенные читатели. И на первый взгляд виноваты сами пользователи, но, как оказалось, не все так однозначно.

Как захватывают ICQ

Если отбросить варианты с банальным и трудоемким подбором паролей к номерам UIN ICQ, то существует один популярный способ «взлома», который срабатывает, если в информационном поле «Номер ICQ и e-mail» программы «светится» бесплатный почтовый адрес владельца (например, blondinka@mail.ru). В этом случае процедура захвата ICQ начинается со «взлома» почтового ящика, ведь к нему можно сгенерировать новый пароль, когда правильно отвечаешь в почтовой системе на вопрос, который владелец ящика назначил для самого себя при регистрации.

Кстати, лидером по популярности является контрольный вопрос «Имя моей любимой собачки», а ответ на него можно выяснить с первой попытки «случайного» знакомства и непродолжительного общения с самим владельцем посредством интернет-пейджера. Дальше все понятно — захватываем почтовый ящик и на сайте www.icq.com просим создать и выслать нам новый пароль к соответствующему номеру.

Но в большинстве случаев краж ICQ-номеров, о которых нам поведали читатели, никаких e-mail-адресов в информационных полях вообще не было указано. И здесь можно все списать на работу «троянских коней» в операционных системах пользователей, как, собственно, и поступают специалисты поддержки этого сервера.

Однако повальные захваты номеров ICQ, принадлежащих известным нам перестраховщикам в плане безопасности, заставили нас задуматься. Сопоставив несколько случаев подбора паролей пользователей ICQ-Rambler, мы пришли к выводу, что возможной причиной таких неприятностей была утечка базы данных учетных записей пользователей с сервера ICQ-Rambler.

Неофициальная версия

Сбой в работе программы ICQ, который многие пользователи могли самостоятельно заметить в начале апреля, был вызван модернизацией системы авторизации на площадках AOL (America Online). Скорее всего именно в процессе программной аварии произошла утечка баз данных программы ICQ, включающих номера UIN и пароли к ним. Разумеется, все было закодировано, но, судя по всему, защищенная информация оказалась взломанной, и теперь на многочисленных хакерских ресурсах по частям выкладываются списки номеров ICQ и пароли к ним.

При этом руководители подразделений ICQ не дают официальных комментариев по поводу многочисленных перехватов пользовательских данных и не спешат на помощь пострадавшим. А на международных сайтах ICQ нет даже намеков на потенциальные проблемы — поразительное безразличие!

Другими словами, пользователи гонят волну негодования на ICQ, те в свою очередь пересылают недовольных людей с их вопросами к ICQ-Rambler. А здесь стрелки переводятся на специалистов компании AOL, которые занимаются технической поддержкой программы ICQ. Вот и все, круг замкнулся, а между тем мошенники пользуются сложившейся ситуацией по своим сценариям.

Чем опасен перехват ICQ

За последние годы сервис ICQ стал универсальным способом общения между людьми во всем мире. И многие активно используют эту программу даже в деловой переписке.

Так вот, не каждый человек удивится, если в один прекрасный день его близкий друг или деловой партнер обратится к нему по «аське» с небольшой деликатной просьбой — одолжить некоторую сумму электронных денег на пару дней. Скорее всего наивный пользователь отнесется к подобной просьбе ответственно, ведь к нему взывает проверенный годами хороший знакомый. Что происходит дальше — понятно.

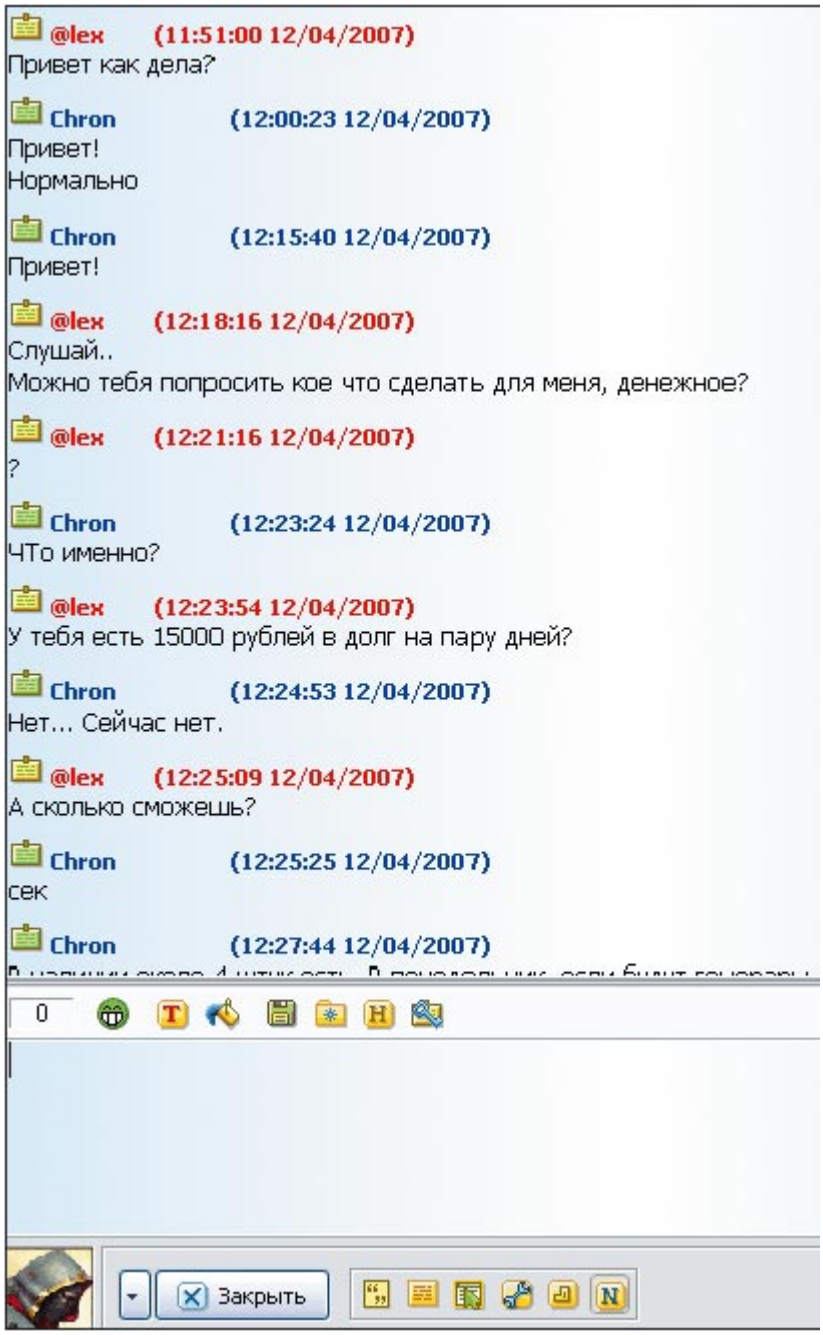
Обычно деньги выпрашиваются в долг в виде карт оплаты Webmoney (возможны варианты с предоплаченными картами сотовых операторов), поскольку эта система имеет развитую сеть по продаже карт и позволяет получателю денег оставаться анонимным на 100%. Далее из системы Webmoney деньги переводятся по цепочке из одной иностранной системы электронных платежей в другую. В результате найти мошенников довольно трудно, и местным отделениям милиции заниматься этим очень не хочется.

Профилактика перехвата ICQ

Прежде всего смените ICQ-пароль сразу после прочтения этой статьи. Учтите, злоумышленники имеют возможность видеть пароли в открытом виде, а значит, поменяйте совпадающие пароли и для других своих ресурсов.

Во-вторых, пропишите в настройках программы ICQ ваш проверенный почтовый ящик и не забудьте поставить галочку запрета отображения адреса e-mail в информационном блоке ICQ. Хотя надежнее воспользоваться программой ICQ-Rambler и завести для себя почтовый адрес SpecialMailBox@rambler.ru, чтобы привязать к нему учетную запись ICQ. Все, теперь можно ассоциированный ящик SecretMailBox удалить из полей ICQ, он все равно останется в специальных записях на сервере, что пригодится для восстановления.

И последнее. Беседуя по ICQ, задумайтесь, стоит ли отвечать на вопросы об имени вашей кошечки или о девичьей фамилии вашей матери. Возможно, вы уже под прицелом интернет-вредителей.



Если это произошло

Если вы не можете авторизоваться в своей программе ICQ по старому паролю либо в процессе работы ICQ появляется сообщение о другом пользователе с таким же UIN, то похоже, что вы уже «в разработке» у злоумышленника и нужно как можно скорее сменить ICQ-пароль. Не получается?

Тогда срочно заходим в почтовый ящик, с которым ассоциирована ваша «аська», и пытаемся уже в почтовой системе оперативно сменить пароль. Если опять не выходит, то расслабляемся и берем телефонную книжку, чтобы начать контрольный обзвон всех близких и знакомых. Кстати, в этом случае с номером ICQ можно попрощаться, специалисты американской компании вряд ли будут пытаться помочь вам в индивидуальном порядке по переписке — на сайте нет даже контактной формы для подобных случаев.

Если же ассоциированный ящик еще под вашим контролем, идем по ссылке https://www.icq.com/password и на втором этапе восстановления ICQ-пароля либо отвечаем на вопросы и вводим спасительный электронный адрес, либо переходим по ссылке «If these are not your questions & answers, click here», чтобы не отвечать на заданные вопросы. Все, теперь в вашу ассоциированную почту придет письмо примерно с таким кодом:

Your confirmation code is:

7BE2CDCC193E9K53243F32FB6E11C6A0D9A03A67F24

6CBE83DB134CB076463A41DE929E3A7D95490651C741A

7F379405F659792994CC237E4E6620CCF5CDEC67E3B462

B7FD54A80D0E4CB8737E30D85BABCD189FE1A060FFBCF

57AAAE4F799B5

The ICQ Password Assistance System.

Не пугайтесь, это не ваш новый пароль (максимальная длина пароля ICQ — восемь символов), просто нужно соответствующий фрагмент автоматического письма вставить в поле кода на сервере ICQ (третий шаг восстановления), и система создаст для вас новый пароль, выкинув из «аськи» злоумышленника.

Вернули интернет-пейджер назад? Тогда не поленитесь сделать информационную рассылку по своему контакт-листу, ведь неизвестно, что успел натворить нехороший человек под вашим именем.

И помните: все следует делать быстро, поэтому порепетируйте операцию восстановления заблаговременно, чтобы запастись необходимыми навыками и проверить статус «прописанного» ICQ primary e-mail. Не забывайте: пострадать могут ваши близкие люди, а кроме того, из-за ущерба, нанесенного ICQ-мошенниками, вы рискуете потерять самых отзывчивых друзей.

Подытоживая разговор

Думаете, в описанной ситуации не можете оказаться вы и ваши знакомые? Не будьте столь самоуверенными, лучше ознакомьтесь с приведенными снимками экранов реальных попыток обмана людей, а также не поленитесь посмотреть на «Мир ПК-диске» подлинный листинг успешной операции мошенника по отношению к продвинутому пользователю. Возможно, вы измените свое представление о безопасности в сети ICQ.